Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2024–2025 **Aanhangsel van de Handelingen**

Vragen gesteld door de leden der Kamer, met de daarop door de regering gegeven antwoorden

2676

Vragen van de leden **Bontenbal** en **Boswijk** (beiden CDA) aan de Ministers van Klimaat en Groene Groei en van Binnenlandse Zaken en Koninkrijksrelaties over *het bericht dat Amerikaanse experts geheime communicatieapparatuur hebben aangetroffen in Chinese zonne-omvormers* (ingezonden 21 mei 2025).

Antwoord van Minister **Hermans** (Klimaat en Groene Groei), mede namens de Ministers van Binnenlandse Zaken en Koninkrijksrelaties, van Economische Zaken en van Justitie en Veiligheid (ontvangen 7 juli 2025). Zie ook Aanhangsel Handelingen, vergaderjaar 2024–2025, nr. 2429.

Vraag 1
Bent u bekend met het artikel «Rogue communication devices found in Chinese solar power inverters»[1]?

Antwoord 1
Ja.

Vraag 2, 3 en 8
Is het feit dat er naar schatting in totaal 200 gigawatt (GW) aan Europese zonne-energiecapaciteit (een vermogen dat gelijk is aan dat van meer dan 200 kerncentrales) is gelinkt aan in China gemaakte omvormers voor u reden tot zorg?
Deelt u de mening dat dit laat zien dat we in Europa te afhankelijk zijn geworden van Chinese omvormers en dat dit grote risico's met zich mee kan brengen voor onze energie-infrastructuur?
Wat zijn de potentiële risico's voor de Nederlandse energievoorziening als ook in (een deel van) deze omvormers geheime communicatieapparatuur is geïnstalleerd?

Antwoord 2, 3 en 8
Er is veel gigawatt aan Europese zonne-energiecapaciteit gelinkt aan Chinese omvormers, en dat is voor het kabinet reden om alert te zijn. Het kabinet en de vitale energieaanbieders brengen de dreigingen in kaart om goed zicht te

[1] Reuters, 14 mei 2025, «Rogue communication devices found in Chinese solar power inverters». (https://www.reuters.com/sustainability/climate-energy/ghost-machine-rogue-communication-devices-found-chinese-inverters-2025-05-14/)

ah-tk-20242025-2676
ISSN 0921 - 7398
's-Gravenhage 2025

houden op de werkelijke risico's voor onze energie-infrastructuur. Omvormers maken hiervan onderdeel uit.
Het Nederlandse energiesysteem wordt beschermd door een robuust ontwerp, redundantie, de aanwezigheid van voldoende herstelcapaciteit en interconnectie met de ons omringende landen. De eventuele risico's van ongedocumenteerde componenten in omvormers voor de Nederlandse energievoorziening zijn afhankelijk van meerdere factoren, zoals: het totaal beschikbare vermogen van de getroffen partij(en) en de (internationale) belastbaarheid van het elektriciteitsnet tijdens een eventuele uitval.
In het aangehaalde artikel staat dat er geheime componenten in omvormers voor zonnepanelen zijn aangebracht, waarmee China op afstand omvormers aan en uit kan schakelen en instellingen kan aanpassen. Dit bericht is gebaseerd op anonieme bronnen en beschrijft niet door wie en hoe het onderzoek is uitgevoerd. Verder is niet aangegeven om welke producten en leveranciers het gaat. Deze informatie is ook niet via andere kanalen beschikbaar gekomen. Omdat deze informatie niet beschikbaar is, kan niet worden vastgesteld of en zo ja waar deze producten in Nederland of Europa worden gebruikt.

Vraag 4
Vallen de zonne-energiecapaciteit en de bijbehorende omvormers onder de vitale objecten waarvan de Algemene Inlichtingen- en Veiligheidsdienst (AIVD) de wettelijke taak heeft maatregelen te bevorderen voor een adequate beveiliging (c-taak)? Ziet de AIVD redenen om naar aanleiding van het genoemde bericht redenen om maatregelen te bevorderen? Zo ja, welke? Zo nee, waarom niet?

Antwoord 4
De AIVD heeft de wettelijke taak om maatregelen te bevorderen ter bescherming van vitale belangen. Zonne-energiecapaciteit en de bijbehorende omvormers kunnen onder deze vitale belangen in de c-taak[2] vallen. De integriteit van omvormers is relevant voor de nationale veiligheid en daarmee de c-taak indien met die omvormers transport, distributie en productie van elektriciteit substantieel kunnen worden verstoord. Dit is aan de orde zodra op grote schaal instellingen van omvormers voor zonnepanelen kunnen worden veranderd of wanneer deze kunnen worden uitgeschakeld.
Voor de nationale veiligheid is het essentieel dat veiligheidsaspecten worden meegenomen bij het aanschaffen en inrichten van nieuwe infrastructuur om daarmee te voorkomen dat er op korte of langere termijn kwetsbaarheden ontstaan die voor grootschalige verstoringen kunnen zorgen. De AIVD draagt deze boodschap onder meer onder de c-taak op verschillende manieren uit. Denk hierbij aan bilaterale contacten met organisaties binnen de vitale infrastructuur en relevante overheidsorganisaties

Vraag 5, 9, 11 en 18
In hoeverre wordt er binnen de Europese Unie (EU) nagedacht over maatregelen om gezamenlijk op te treden tegen de import en het gebruik van potentieel onveilige Chinese omvormers? Wordt er bijvoorbeeld overwogen om in navolging van Litouwen het gebruik van deze omvormers in installaties boven een bepaalde capaciteit te verbieden?
Welke waarborgen en controles zijn er om te voorkomen dat dergelijke apparatuur wordt geïnstalleerd in bijvoorbeeld omvormers die ook in Nederland worden gebruikt?
Is bestaande wet- en regelgeving die ervoor moet zorgen dat ook fabrikanten en leveranciers hun verantwoordelijkheid nemen om de risico's van door hen geleverde apparatuur voor het elektriciteitsnet te verkleinen voldoende om te voorkomen dat er alsnog bijvoorbeeld geheime communicatieapparatuur in wordt geïnstalleerd?
Kunt u uiteenzetten hoe er bij de implementatie van deze Europese richtlijnen die gaan over het verbeteren van de bescherming van vitale infrastructuur in Nederland aandacht wordt besteed aan verbeterde beveiliging van zonne-omvormers en andere componenten van het elektriciteitsnet?

[2] artikel 8, lid 2c Wiv2017

Antwoord 5, 9, 11 en 18
Vraag 9 heeft betrekking op geheime communicatieapparatuur «dergelijke apparatuur».
Vraag 18 heeft betrekking op de NIS2- en de CER- richtlijnen «deze Europese richtlijnen».
Omvormers moeten voldoen aan elektrotechnische eisen die in de Netcode Elektriciteit[3] staan, die deels voortvloeien uit de Europese Netcode «Requirements for Generators[4]». Omvormerfabrikanten moeten met een door een onafhankelijk geaccrediteerd testbureau verstrekt testcertificaat aantonen dat zij voldoen aan de functionele vereisten uit deze Netcode. Netbeheerders houden hier toezicht op.
Bedrijven die actief zijn in de elektriciteitssector, gebruikmaken van omvormers en onder de Wet beveiliging netwerk- en informatiesystemen (Wbni) vallen, zijn verplicht beveiligingsmaatregelen te nemen. De Rijksinspectie Digitale Infrastructuur (RDI) houdt hier toezicht op. Op korte termijn worden deze wettelijke verplichtingen uitgebreid middels de Cyberbeveiligingswet (Cbw) en de toekomstige Wet weerbaarheid kritieke entiteiten (Wwke). KGG heeft uitvoerig contact met bedrijven over de uitvoering van deze toekomstige wetgeving.
Met de komst van de Cbw en Wwke worden zwaardere beveiligingseisen gesteld dan voorzien in de huidige Wbni. Bedrijven moeten op basis van een risicogebaseerde aanpak zorgdragen voor de beveiliging van hun netwerk- en informatiesystemen. Bij het overwegen van passende maatregelen zijn bedrijven verplicht om rekening te houden met de specifieke kwetsbaarheden van hun rechtstreekse leveranciers en dienstverleners en met de algemene kwaliteit van de producten en de cyberbeveiligingspraktijken van hun leveranciers en dienstverleners.
Voor mogelijke cyberrisico's van zonne-omvormers gebruikt door consumenten en bedrijven zijn er additionele wetgevingstrajecten die gericht zijn op de fabrikanten van hard- en software. Voor digitale producten op de Europese markt introduceren de gedelegeerde handeling onder de radioapparatuurrichtlijn (RED3.3def) en de Cyber Resilience Act (CRA) cybersecurityeisen waaraan deze producten moeten voldoen. Vanaf augustus 2025 is de RED3.3def van kracht met eisen voor alle draadloos verbonden apparaten, waaronder zonnepaneelomvormers. Vanaf december 2027 is de CRA van kracht met eisen voor alle producten met digitale elementen (hardware- en softwareproducten), waaronder zowel consumentenapparatuur en -software, als digitale producten voor industriële en operationele toepassingen vallen. Fabrikanten, importeurs en distributeurs mogen op grond van deze productregelgeving alleen producten op de EU-markt aanbieden die passende beveiligingsmaatregelen bevatten. Deze maatregelen hebben onder meer betrekking op ongeautoriseerde toegang. Producten moeten passend beveiligd zijn tegen hacken.
Op de Europese markt is het verboden om (heimelijk) functionaliteit in te bouwen (zowel software en hardware) die niet in de technische documentatie is beschreven. Het is verboden om producten aan te bieden die «verstopte» functionaliteiten bevatten om apparaten op afstand aan of uit te zetten. Deze eisen gelden ook voor producten die afkomstig zijn van een fabrikant die buiten de EU is gevestigd, zodra deze producten op de Europese markt worden aangeboden.
De RDI houdt toezicht op deze wettelijke verplichtingen. De RDI onderzoekt onder meer op basis van steekproeven in testlaboratoria of de producten overeenkomen met de technische documentatie en of de producten de nodige cybersecuritymaatregelen bevatten. Vooruitlopend op de inwerkingtreding van deze cybersecurityproducteisen heeft de RDI in 2023 een rapport gepubliceerd over zonnepaneelomvormers waarin fabrikanten op deze aankomende verplichtingen worden gewezen.[5]
Het kabinet acht deze combinatie van product- en ketengerichte Europese wetgeving essentieel om risico's te beheersen en de weerbaarheid van het Europese energiesysteem te versterken.

---

[3] Netcode elektriciteit
[4] Code Requirements for Generators
[5] Onderzoek storingsproblematiek en cyberveiligheid omvormers RDI 2023

De aangehaalde regelgeving in Litouwen is bedoeld om de digitale toegang tot apparatuur met een capaciteit van meer dan 100 kW te beperken. De meerderheid van de Nederlandse consumenten PV-installaties heeft een kleinere capaciteit en zou niet onder de reikwijdte van dergelijke regelgeving vallen. Het kabinet is geïnformeerd over het bestaan van deze regelgeving. Het kabinet zal, in samenwerking met onze partners binnen de Europese Unie, de komende tijd bezien of dergelijke voorschriften toegevoegde waarde hebben voor de Europese markt.

Vraag 6
Welke initiatieven zijn er nationaal en in Europees verband om Europese fabrikanten van veilige en betrouwbare omvormers te ondersteunen en het gebruik van in Europa geproduceerde omvormers te stimuleren en daarmee de afhankelijkheid van Chinese producten te verminderen?

Antwoord 6
Zowel op nationaal als op Europees niveau lopen er verschillende initiatieven om Europese fabrikanten van omvormers te ondersteunen en risicovolle strategische afhankelijkheden van China te verminderen. De EU investeert in de ontwikkeling en opschaling van Europese productiecapaciteit, technologische innovatie en het formuleren van strengere (veiligheids-) normen. De Net-Zero Industry Act (NZIA) heeft als doel om de Europese netto-nultechnologieën op te schalen naar ten minste 40% van de jaarlijkse Europese behoefte in 2030. De EU streeft ernaar om rond 2030 productiecapaciteit te hebben om zelf minstens 40% van de omvormers te kunnen produceren die jaarlijks nodig zijn voor het behalen van haar klimaat- en energiedoelen.
Deze doelen worden ondersteund via het Europees publiek-privaat samenwerkingsinstrumentarium zoals Important Projects of Common European Interest (IPCEI), en onderzoekprogramma's zoals Horizon Europe. Nederland neemt hieraan actief deel.
Voor Nederland heeft Invest-NL in samenwerking met TKI Urban Energy in kaart gebracht wat nodig is om een sterke Europese basis voor de productie van zonnepanelen te realiseren en strategische onafhankelijkheid te bereiken[6]. Nationaal wordt er gewerkt aan verschillende maatregelen ter bevordering van circulaire zonnestroomsystemen, zoals beschreven in het Nationaal Programma Circulaire Economie (NPCE), initiatieven die lopen via Topsector Energie en industriële programma's binnen het Nationaal Groeifonds.

Vraag 7
Kunt u aangeven in hoeverre en op welke schaal omvormers van Chinese makelij momenteel in Nederland zijn geïnstalleerd?

Antwoord 7
In onder meer het rapport «Scenario's en maatregelen voor cyberweerbare zonnestroominstallaties» staat dat een substantieel deel van de in Nederland geïnstalleerde omvormers afkomstig is van Chinese fabrikanten[7]. Dit rapport is opgesteld in opdracht van de Rijksdienst voor Ondernemend Nederland en Topsector Energie. Dit rapport beschrijft zowel residentiële toepassingen als grootschalige zonneparken.

Vraag 10
In hoeverre bestaan er in Nederland en in de EU systemen of procedures waarmee verdachte communicatie vanuit omvormers kan worden gedetecteerd of geblokkeerd? Worden daar actief controles op uitgevoerd?

Antwoord 10
De RDI heeft haar inspecties geïntensifieerd en is in gesprek met fabrikanten om hun producten te verbeteren en voor te bereiden op de RED- en CRA-verplichtingen.

---

[6] https://solarmagazine.nl/nieuws-zonne-energie/i39444/27-miljard-euro-nodig-voor-europese-productie-zonnepanelen
[7] Scenario's en maatregelen voor cyberweerbare zonnestroominstallaties augustus 2024

Omvormers voor zonnepanelen zijn veelal consumentenproducten die communiceren via cloudplatforms van de fabrikant. Er is geen systeem om het volledige dataverkeer en potentieel (verdachte) communicatie te herkennen of te blokkeren. Misbruik van deze platforms en cyberdreigingen wordt internationaal gemonitord. Cloudplatformen hebben in de eerste plaats zelf mogelijkheden om cyberdreigingen te monitoren en te mitigeren. Ook de overheid heeft een taak. In Nederland is het Nationaal Cyber Security Centrum hier medeverantwoordelijk voor. Het Nationaal Cyber Security Centrum reageert op cyberincidenten, geeft advies en bevordert de publiek-private samenwerking rond cloudplatforms.
Zodra de CRA van kracht is, gelden er meer cybersecurityvereisten voor omvormers voor zonnepanelen, inclusief de applicaties waarmee deze kunnen worden bediend. Ook de gegevensverwerking op afstand via clouddiensten van de fabrikant moet voldoen aan de cyberveiligheidseisen, waaronder bescherming tegen ongeautoriseerde toegang. Deze cloudcomponenten moeten ook beschreven staan in de technische documentatie. De toezichthouder kan zowel administratief als in de praktijk toezicht houden. De RDI zou toegang kunnen vorderen tot de productie omgeving, van een cloudplatform, om controles uit te voeren.

Vraag 12
Hoe groot acht u het risico dat kwaadwillende actoren via ongeautoriseerde communicatieapparatuur in zonne-omvormers gecoördineerde verstoringen kunnen veroorzaken in het Nederlandse elektriciteitsnet, bijvoorbeeld door duizenden huishoudens of installaties tegelijkertijd uit te schakelen?

Antwoord 12
De aanwezigheid van hardwarecomponenten, zoals bijvoorbeeld een 5g-verbinding via een ingebouwde communicatiemodule, zoals geopperd in het Reuters artikel (dat spreekt van «devices») wordt niet praktisch geacht en is in de praktijk goed te detecteren door de toezichthouder.
Zodra een module wel is opgenomen in de technische documentatie moet deze op grond van de RED3.3 passend beveiligd zijn tegen ongeautoriseerde toegang (hacken door derden).
Het kabinet neemt dergelijke signalen desalniettemin zeer serieus. Juist vanwege de toenemende digitalisering en het gebruik van slimme apparatuur, zoals omvormers, is de nationale en Europese wetgeving aangescherpt. Op alle schakels in de keten is er aandacht voor cybersecurity.
Zowel het Nationaal Cyber Security Centrum, de Rijksinspectie Digitale Infrastructuur als publiek-private organisaties zoals de Topsector Energie en branchevereniging Holland Solar zetten in op de weerbaarheid van de energiesector, inclusief consumentenapparaten. Leveranciers en exploitanten worden aangesproken op hun verantwoordelijkheid om apparatuur veilig in te richten, verdachte patronen te monitoren en zich te verenigen om gezamenlijk de weerbaarheid van deze apparaten te versterken.

Vraag 13, 14, 15 en 16
Welke maatregelen zijn er genomen sinds de waarschuwing van de Rijksinspectie Digitale Infrastructuur (RDI) van mei 2023[8] over de kwetsbaarheid van zonne-omvormers voor hacking en sabotage?
Welke stappen zijn er specifiek gezet naar aanleiding van de bevinding van de RDI dat geen enkele van de onderzochte omvormers voldeed aan de norm en daardoor eenvoudig was te hacken, van afstand uit te schakelen of in te zetten voor DDoS-aanvallen?
Heeft de RDI hier in de afgelopen twee jaar nieuw onderzoek naar gedaan en is daarbij verbetering geconstateerd?
Heeft het onderzoek van de RDI uit 2023 ertoe geleid dat er een bredere evaluatie is uitgevoerd van bestaande zonne-energie-installaties in Nederland om te bepalen welke omvormers mogelijk een beveiligingsrisico vormen? Zo ja, wat zijn daarvan de resultaten en welke vervolgstappen worden er

[8] Rijksinspectie Digitale Infrastructuur, 30 mei 2023, «Omvormers kunnen storing veroorzaken en zijn vaak makkelijk te hacken». (https://www.rdi.nl/actueel/nieuws/2023/05/30/omvormers-kunnen-storing-veroorzaken-en-zijn-vaak-makkelijk-te-hacken)

genomen? Zo nee, bent u bereid om hier alsnog vervolgonderzoek naar te laten doen?

Antwoord 13, 14, 15 en 16
Uit het onderzoek van RDI uit 2023 bleek dat de kwetsbaarheden vooral zitten in de slechte beveiliging van omvormers door het gebruik van standaard wachtwoorden en in het niet tijdig zorgen voor software-updates door fabrikanten om de omvormers veilig te houden. De RDI heeft in de periode 2023–2024 geen vervolgonderzoek uitgevoerd naar de cyberveiligheid van omvormers voor zonnepanelen.
De RDI heeft haar inspecties geïntensiveerd, en fabrikanten aangemoedigd om hun producten te verbeteren en voor te bereiden op de RED- en CRA-verplichtingen. Er wordt gewerkt aan normontwikkeling op Europees niveau, ook met het oog op certificering en producttoelating. Mede daarom is de relatie met importeurs en distributeurs verdiept en wordt er, via marktonderzoek, steekproefsgewijs gecontroleerd of apparaten voldoen aan de technische documentatie.
De fabrikant, de installateur en de consument hebben een eigen verantwoordelijkheid om de zonnestroominstallaties te allen tijde goed te beveiligen met sterke wachtwoorden en door regelmatig updates uit te voeren. In de Gedragscode Zon op Woningen heeft de sector afspraken gemaakt over het veilig installeren van residentiële systemen. Volgens deze gedragscode zal de installateur de omvormer instellen met een sterk en per installatie uniek wachtwoord voor de onderhoudsinstellingen van de omvormer.
Verder werkt het kabinet aan proactieve informatieverstrekking over de komende wet -en regelgeving, zodat de partijen en fabrikanten zich alvast kunnen voorbereiden. Het kabinet zet ook in op het vergroten van bewustzijn, zoals in de overheidscampagne «Doe je updates», waarin een oproep wordt gedaan om slimme apparaten in huis direct te updaten.
Vanwege de in het onderzoek beschreven risico's was en is het zaak dat fabrikanten hun apparaten waar nodig aanpassen. RDI ziet erop toe dat fabrikanten deze maatregelen nemen. Dit doet zij door controles te doen vanaf 1 augustus 2025 wanneer deze eisen in werking treden. Als hieruit blijkt dat fabrikanten in de producten die zij na die datum op de markt aanbieden geen passende maatregelen hebben genomen, kan de RDI handhavende maatregelen nemen. Dit zijn eerste lichte maatregelen, die opgebouwd kunnen worden naar bijvoorbeeld boetes, verkoopverboden of terugroepacties.

Vraag 17
Hoe verloopt de implementatie van de Critical Entities Resilience Directive (CER) en de Network- and Information Security 2 Directive (NIS2) in Nederland?